

AUG 02 2006

REMARKS

Claims 1-3, 5-7, 9-17, 19-21, 23-30, and 33-38 are pending and stand rejected. In this response, Claims 1, 5, 10, 13, 14, 15, 19, 24, 27, 28, 29, 33, 34, 37, and 38 have been amended, and Claims 8 and 22 been cancelled. Based on the amendments and the following remarks, the Applicants respectfully request that the Examiner withdraw the rejections and pass the application on to issuance.

Claim Objections: Claim 34 has been amended to address the Examiner's concerns.

Claim Rejections – 35 USC §103: The Examiner rejected Claims 1-3, 6, 7, 11, 12, 15-17, 20, 21, 25, and 26 under §103 as being unpatentable over USPN 6,453,127 issued to Wood in view of USPN 6,154,843 issued to Hart. To establish a prima facie case of obviousness, the Examiner must show some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; that there is a reasonable expectation of success; and that the prior art reference (or references when combined) teach or suggest all the claim limitations. MPEP § 2142.

As is made clear below, The Examiner has not established a prima facie case for obviousness as Wood and Hart fail to teach one or more elements of each of Claims 1-3, 6-8, 11, 12, 15-17, 20-22, 25, and 26.

Claims 1 and 15: Claim 1 is directed to a method for mediating access to production options and (as amended) recites the following acts.

1. acquiring a user's access request for a production device;
2. accessing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document;

3. in response to the user's access request, dynamically generating a user interface according to the accessed data so that the user interface provides user accessible controls for only those options for which the user has permission to access; and
4. presenting the user with the generated user interface so that through the user interface the user can cause the production of the target document by the production device in accordance with a selection of one or more of the user accessible controls provided by the user interface.

Claim 15 is directed to a computer program product that includes a computer useable medium having computer readable instructions for performing the elements listed above.

The Examiner mistakenly asserts that Wood, column 6, lines 1-8, teaches accessing data representing the production options to which the particular user does and/or does not have permission to access. Claims 1 and 15 have been amended to recite that the data at least indirectly identifies those production options to which the user does not have permission to access.

The passage cited by the Examiner is reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10. Even a cursory review of the cited passage reveals that Wood mentions nothing of accessing data that at least indirectly identifies those production options to which the user does not have permission to access. The passage merely describes web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. Hart is silent on this point.

Consequently, Wood and Hart fail to teach or suggest accessing data that at least indirectly identifies those production options to which the user does not have permission to access where each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document. For at least this reason, Claims 1 and 15 are patentable over the cited references as are Claims 2, 3, 5-7 and 9-12 which depend from Claim 1 and Claims 16, 17, 19-21, and 23-26 which depend from Claim 15.

Claim Rejections – 35 USC §103: The Examiner rejected Claims 5, 9, 10, 13, 14, 19, 23, 24, 27-30, 33, and 34 under §103 as being unpatentable over Wood in view of Hart and in further view of USPN 6,751,657 issued to Zothner.

Claims 5, 9, and 10 each depend from Claim 1 and are patentable over the cited references based at least on their dependence from Claim 1.

Claims 13 and 27: Claim 13 is directed to a method for mediating access to production options and recites the following:

1. acquiring a user's access request for a production device;
2. accessing a record established for the user, the record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document;
3. generating a web page for the production device according to the user's record so that the user interface provides user accessible controls for only those options for which the user has permission to access; and
4. presenting the user with the generated web page so that through the web page the user can cause the production of the target document by the production device in accordance with a selection of one or more of the user accessible controls provided by the user interface.

Claim 27 is directed to a computer program product that includes a computer useable medium having computer readable instructions for performing the elements listed above.

The Examiner asserts that Wood, column 6, lines 1-8 and Zothner, column 9, line 64 through column 10, line 8 teaches accessing data representing production options to which the user does and/or does not have permission to access. Claims 13 and 27 have been amended to recite that the data at least indirectly identifies those production options to which the user does not have permission to access.

The passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of accessing a record established for the user where that record contains data that at least indirectly identifies those production options to which the user does not have permission to access. The passage from Wood merely describes

web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly, Hart is silent on this point.

Consequently, Wood, Zothner, and Hart fail to teach or suggest accessing a record established for the user, the record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document. For at least this reason, Claims 13 and 27 are patentable over the cited references.

Claims 14 and 28: Claim 14 is directed to a method for mediating access to production options and recites the following:

1. acquiring a user's access request for a production device;
2. retrieving a web page for the production device, the web page having user accessible controls for selecting production options;
3. accessing a record established for the user, the record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document; and
4. altering the web page according to the user's record so that the web page provides user accessible controls for only those options for which the user has permission to access; and
5. presenting the user with the modified web page so that through the web page the user can cause the production of the target document by the production device in accordance with a selection of one or more of the user accessible controls provided by the user interface..

Claim 28 is directed to a computer program product that includes a computer useable medium having computer readable instructions for performing the elements listed above.

The Examiner asserts that Wood, column 6, lines 1-8 and Zothner, column 9, line 64 through column 10, line 8 teaches accessing data representing production options to which the user does and/or does not have permission to access. Claims 14 and 28 have been amended to recite that the data at least indirectly identifies those production options to which the user does not have permission to access.

The passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of accessing a record established for the user where that record contains data that at least indirectly identifies those production options to which the user does not have permission to access. The passage from Wood merely describes web content for displaying a log-in page. That web content does not identify

production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly, Hart is silent on this point.

Consequently, Wood, Zothner, and Hart fail to teach or suggest accessing a record established for the user, the record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document. For at least this reason, Claims 14 and 28 are patentable over the cited references.

Claims 19, 23, and 24 each depend from Claim 15 and are patentable over the cited references based at least on their dependence from Claim 15.

Claim 29 is directed to a system for managing electronic document production, and, as amended, recites the following elements.

1. a production server operable to dynamically generate an interface according to a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document;
2. a permission service in operable to acquire a client's access request for the production device and in response to direct the production server to generate an interface according to the user's record so that the user interface provides user accessible controls for only those options for which the user has permission to access, and to direct to the client the generated interface so that through the interface the user can cause the production of the target document by the selected production device in accordance with a selection of one or more of the user accessible controls provided by the modified interface.

The Examiner mistakenly asserts that Wood, Figure 2, item 30, column 5, lines 3-24, column 6, lines 1-8 and Zothner column 9, line 64 through column 10, line 8 teaches a production server operable to dynamically generate an interface according to a user's record containing data representing the production options for the production device to which the user does and/or does not have permission to access. Claim 29 has been amended to recite that the user record contains data that at least indirectly identifies those production options to which the user does not have permission to access.

Item 30 in Wood's Figure 2 represents a web server computer. The Examiner equates this web server computer with the production server recited in Claim 29. Wood, column 5, lines 5-34 describe the basic operation of any web server computer and mentions nothing of user records containing data identifying production options, directly or indirectly.

The remaining passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of a system component that is operable to dynamically generate an interface according to a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to. The passage from Wood merely describes web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly. Hart is silent on this point.

Consequently, Wood, Zothner, and Hart fail to teach or suggest a production server operable to dynamically generate an interface according to a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to access. For at least this reason, Claim 29 and Claim 30 which depends from Claim 29 are patentable over the cited references.

Claim 33: Claim 33 is directed to a system for managing electronic document production and, as amended, recites the following elements:

1. a production server operable to serve to a client an interface having user accessible controls for selecting production options for a target document, each production option corresponding to feature that when implemented affects a manner in which a selected production device produces a target document;
2. a permission service operable to retrieve the interface from the production server for the selected production device, access a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to access, modify the interface according to the user's record so that the modified interface has user accessible controls for only those options for which the user has permission to access, and direct to the client the modified interface so that through the interface the user can cause the production of the target document by the selected production device in accordance with a selection of one or more of the user accessible controls provided by the modified interface.

The Examiner mistakenly asserts that Wood, column 5, lines 3-24, column 6, lines 1-8 and Zothner column 9, line 64 through column 10, line 8 teaches a permission service operable to retrieve the interface from the production server for the selected production device, access a user's record containing data representing production options to which the user does and/or does not have permission to access. Claim 33 has been amended to recite that the user record contains data that at least indirectly identifies those production options to which the user does not have permission to access.

Wood, column 5, lines 5-34 describe the basic operation of any web server computer and mentions nothing of user records containing data identifying production options, directly or indirectly. The remaining passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of a system component that is operable to dynamically generate an

interface according to a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to. The passage from Wood merely describes web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly. Hart is silent on this point.

Consequently, Wood, Zothner, and Hart fail to teach or suggest a permission service operable to retrieve the interface from the production server for the selected production device, access a user's record containing data that at least indirectly identifies those production options to which the user does not have permission to access. For at least this reason, Claim 33 and Claims 34-36 which depend from Claim 33 are patentable over the cited references.

Claim Rejections – 35 USC § 103: The Examiner rejected Claims 35-38 under § 103 as being unpatentable over Wood in view of Hart and in further view of Zothner and in further view of USPN 6,092,078 issued to Adolfsson.

Claims 35 and 36 each depend from Claim 33 and include all of the limitations of that base claim. For at least the same reasons Claim 33 is patentable, so are Claims 35 and 36.

Claim 37: Claim 37 is directed to a system for a system for managing electronic document production and, as amended, recites the following elements.

1. a production device;
2. one or more user records, each user record containing data that at least indirectly identifies those production options to which the user does not have permission to access, each production option corresponding to feature that when implemented affects a manner in which the production device produces a target document;

3. a production server in communication with the production device and operable to generate an interface for that production device according to a user record so that the generated interface has user accessible controls for only those options for which the user has permission to access;
4. a permission service operable to access the user's record, direct the production server to generate an interface for the production device according to the user's record, and to direct to a client the generated interface so that through the interface the user can cause the production of the target document by the selected production device in accordance with a selection of one or more of the user accessible controls provided by the modified interface;
5. one or more device records, each device record containing data representing the production options offered by the production device;
6. a permission engine operable to parse the device records and generate an web page for managing user records;
7. a device locator operable to detect new production devices; and
8. an update service operable to create a device record for each newly detected production device.

The Examiner mistakenly asserts that Wood, column 6, lines 1-8 and Zothner, column 9, line 64 through column 10, line 8 teaches a system that includes one or more user records, each user record containing data that at least indirectly identifies those production options to which the user does not have permission to access. Claim 37 has been amended to recite that the user records contain data that at least indirectly identifies those production options to which the user does not have permission to access.

The passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java

Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of a user record that contains data that at least indirectly identifies those production options to which the user does not have permission to. The passage from Wood merely describes web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly. Hart and Adolfsson are silent on this point.

Consequently, Wood, Zothner, Hart and Adolfsson fail to teach or suggest one or more user records, each user record containing data that at least indirectly identifies those production options to which the user does not have permission to access. For at least this reason, Claim 37 is patentable over the cited references.

Claim 38: Claim 38 is directed to a system for managing electronic document production and includes the following combination of elements:

1. a production device;
2. one or more user records, each user record containing, for each production device, data that at least indirectly identifies those production options to which the user does not have permission to access, each production option

- corresponding to feature that when implemented affects a manner in which the production device produces a target document;
3. a production server in communication with the production device and operable to serve an interface for that production device, the interface having user accessible controls for selecting production options for the production device;
 4. a permission service operable to access the user's record, retrieve the interface from the production server, modify the interface according to the user's record so that the modified interface has user accessible controls for only those options for which the user has permission to access, and to direct to a client the modified interface so that through the modified interface the user can cause the production of the target document by the selected production device in accordance with a selection of one or more of the user accessible controls provided by the modified interface;
 5. one or more device records, each device record containing data representing the production options offered by the production device;
 6. a permission engine operable to parse the device records and generate an web page for managing user records;
 7. a device locator operable to detect new production devices; and
 8. an update service operable to create a device record for each newly detected production device.

The Examiner mistakenly asserts that Wood, column 6, lines 1-8 and Zothner, column 9, line 64 through column 10, line 8 teaches a system that includes one or more user records, each user record containing data that at least indirectly identifies those production options to which the user does not have permission to access. Claim 38 has been amended to recite that the user records contain data that at least indirectly identifies those production options to which the user does not have permission to access.

The passages cited by the Examiner are reproduced as follows.

The web server 32 then downloads an HTML document and a Java applet from an HTML document and Java files 38, step 130. The Java applet may be an application program for enabling display of the downloaded

document, which could be an initial printer screen page providing a prompt for the user to input an identification (ID) code to provide access to the copier/printer where user authorized codes are required. The Java Virtual Machine in step 140 executes the Java applet, step 140, to enable the remote workstation to display the initial display page.

Wood, col. 6, lines 1-10.

Each UserProfile inherits this basic information from a User object and carries login and customized information. Furthermore, each UserProfile is assigned a Role, which is used to control security accesses and permissions. The User Manager 221 provides handling of user login/logout to the NCMS 101. In addition, the User Manager 221 performs creation, management, and removal of roles and user profiles. The User Manager 221 also retrieves information that is captured in each user profile. The User Manager 221 locks and unlocks the user profiles (i.e., inactivate/reactivate user accounts).

Zothner, col. 9, line 64 through col. 10, line 8.

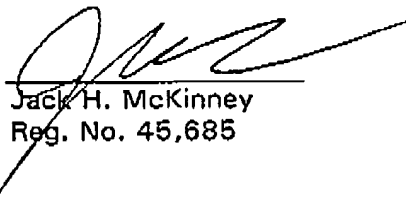
Even a cursory review of the cited passages reveals that Wood and Zothner mention nothing of a user record that contains data that at least indirectly identifies those production options to which the user does not have permission to. The passage from Wood merely describes web content for displaying a log-in page. That web content does not identify production options, directly or indirectly. The passage from Zothner discusses user profiles but mentions nothing of data identifying production options, directly or indirectly. Hart and Adolfsson are silent on this point.

Consequently, Wood, Zothner, Hart and Adolfsson fail to teach or suggest one or more user records, each user record containing data that at least indirectly identifies those production options to which the user does not have permission to access. For at least this reason, Claim 38 is patentable over the cited references.

Conclusion: In view of the foregoing remarks, the Applicant respectfully submits that the pending claims are in condition for allowance. Consequently, early and favorable action allowing these claims and passing the application to issue is earnestly solicited. The foregoing is believed to be a complete response to the outstanding Office Action.

Respectfully submitted,
Shell Sterling Simpson, et al.

By


Jack H. McKinney
Reg. No. 45,685

August 2, 2006